Wireless Hacking

Agenda

- Introducción
- Tecnologías Wireless: Clasificación
- Dispositivos Wireless
- Mecanismos de autenticación WEP y WPA
  - Autenticación Abierta
  - Autenticación por PSK
  - Autenticación por Dirección MAC
- Wireless Sniffers y Localización de SSIDs
- Rogue Access Points
- Comprendiendo las Técnicas de Wireless Hacking
- Pasos para realizar un ataque a una WLAN
- Obtención de clave WEP bajo Linux
- Métodos utilizados para securizar redes Wireless

Introducción

- Las redes wireless son cada día más populares.

- La popularidad de esta tecnología se debe a varios factores:
  - Cobertura geográfica
  - Simplicidad de implementación
  - Costo

- Una red de área local wireless (WLAN) permite a los trabajadores acceder a los recursos informáticos sin necesidad de tener que estar en sus escritorios.

Introducción (Cont.)

- Las redes inalámbricas agregan otro punto de ataque a la red corporativa.
- Dado que es una tecnología relativamente nueva, todavía hay muchos puntos para mejorar.
- Debido a la naturaleza de las ondas RF y a la rápida penetración de esta tecnología en las redes hogareñas y corporativas, existe una gran cantidad de vulnerabilidades y exploits para las mismas.

Introducción (Cont.)

- La mayoría de las WLANs está basadas en el estándar IEEE 802.11 y derivados, como por ejemplo 802.11a, 802.11b, 802.11g y 802.11n.
- En un principio este estándar solo incluía el protocolo de seguridad WEP, el cual era muy limitado y fue explotado con facilidad.
- Para paliar estas debilidades, el IEEE desarrolló la norma 802.11i orientada a cubrir las necesidades de seguridad que las redes wireless demandaban.

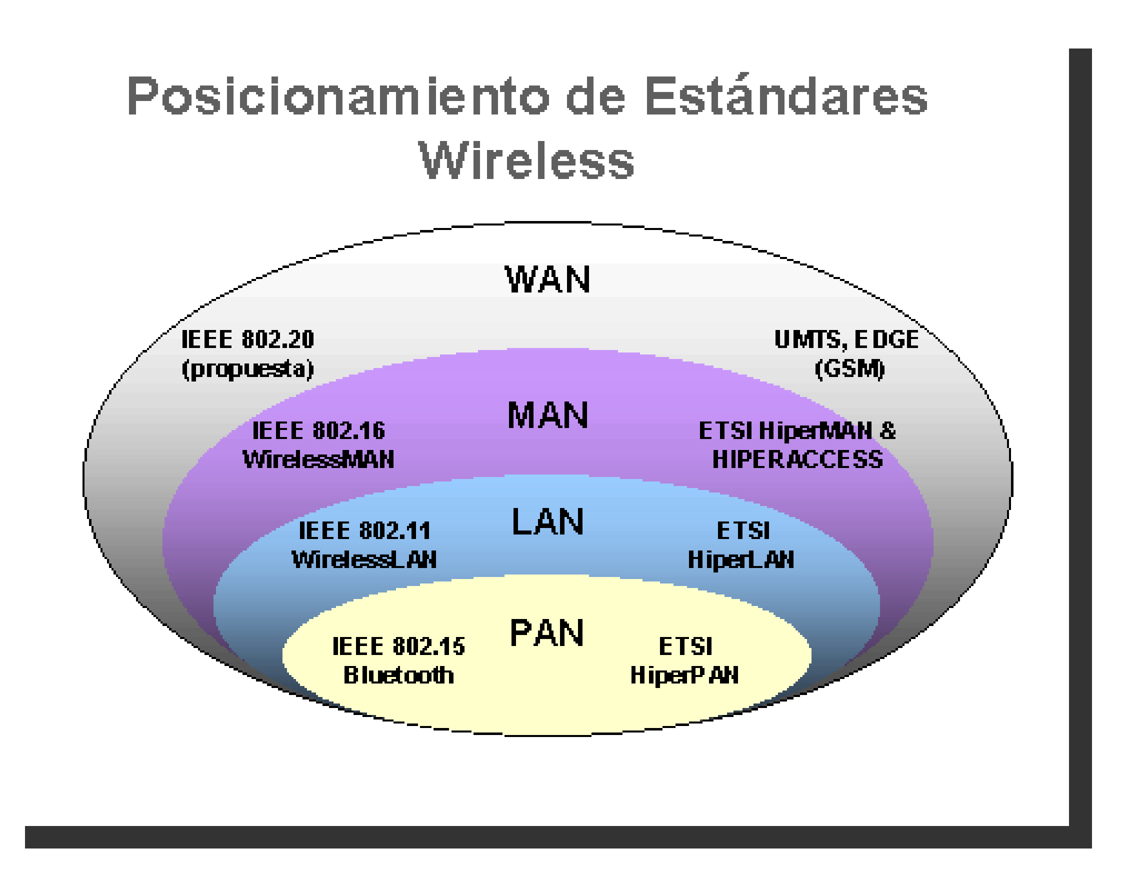
Introducción (Cont.)

- Pero mientras este se desarrollaba, se intentó mejorar el estándar anterior para cubrir la brecha entre el estándar original y la nueva norma.

- La WiFi Alliance creó estadíos de seguridad intermedios conocidos como WPA (WiFi Protected Access) y WPA2 desarrollados ambos para cubrir dicha brecha hasta que el estándar 802.11i estuviese aprobado como estándar por IEEE.

Tecnologías Wireless: Clasificación

- Según el alcance, pueden clasificarse en:
  - WPAN – Wireless Personal Area Network (alcance < 10m)
    - Bluetooth/Infrarrojo
  - WLAN – Wireless LAN
    - WiFi (802.11)
    - WiMax (802.16) (MAN)
  - WWAN – Wireless WAN
    - GPRS/EDGE/3GSM



Tecnologías Wireless: Clasificación (Cont.)

- Por el tipo de acceso, se pueden clasificar en:
  - Modo Ad-Hoc
  - Modo Infraestructura
  - Múltiples puntos de acceso

Modo Ad-Hoc

- Modo Ad-Hoc - También llamadas Independent Basic Service Set (IBSS)

- Se establece una conexión entre dos equipos directamente

- Funcionamiento independiente mientras estén dentro del área que cubre cada uno

- Cada cliente tendría únicamente acceso a los recursos de otro cliente pero no a un servidor central

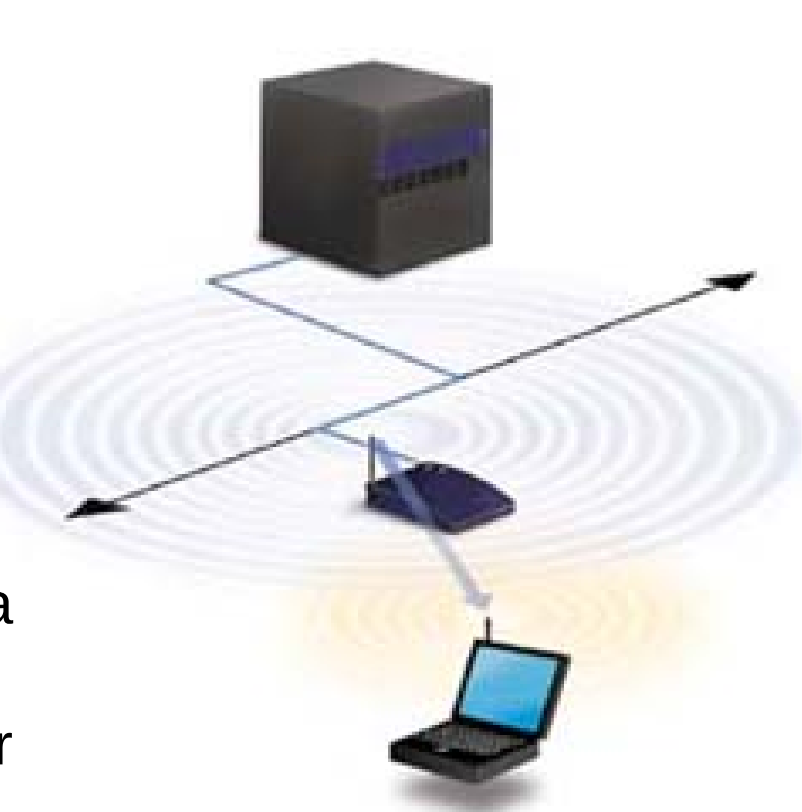
Modo Infraestructura

- Modo Infraestructura - También llamadas Basic Service Set (BSS)

- Un *Access Point* (AP) puede aumentar el rango de comunicación, ya que también actúan como repetidores

- Desde que el *Access Point* se conecta a la red cableada cualquier cliente que tenga acceso a los recursos del servidor puede acceder al mismo

- Cada *Access Point* puede servir a varios clientes



Múltiples Puntos de Acceso

- Múltiples puntos de acceso - También llamada Extended Service Set (ESS)
- Los AP tienen un rango finito
  - Alrededor de 150m en lugares cerrados y 300m en zonas abiertas
- Para cubrir zonas más amplias se necesitan varios AP
- El objetivo es cubrir el área con celdas que solapen sus áreas para poder moverse sin cortes (Roamming)



Estándar IEEE 802.11

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F - Inter-Access Point Protocol (2003)
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)
- IEEE 802.11k - Radio resource measurement enhancements
- IEEE 802.11l - (reserved, typologically unsound)
- IEEE 802.11m - Maintenance of the standard; odds and ends.
- IEEE 802.11n - Higher throughput improvements
- IEEE 802.11o - (reserved, typologically unsound)
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
- IEEE 802.11q - (reserved, typologically unsound, can be confused with 802.1q VLAN trunking)
- IEEE 802.11r - Fast roaming
- IEEE 802.11s - ESS Mesh Networking
- IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics
- IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless network management
- IEEE 802.11w - Protected Management Frames

Dispositivos Wireless

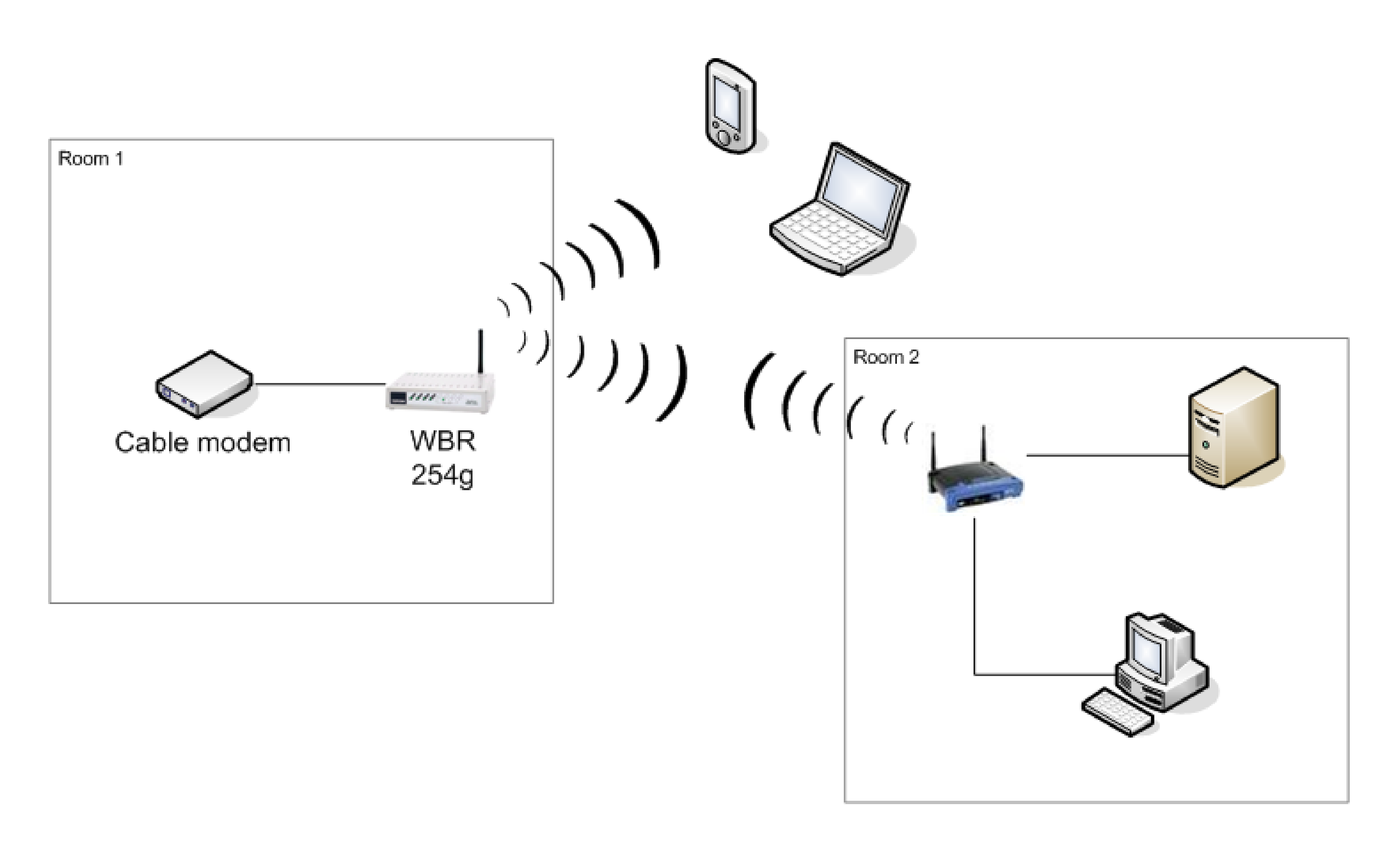
- Access Point
- Bridges / Repetidores
- Wireless card
  - PCI
  - PCMCIA
  - USB Dongles
- Antenas
  - Yagi
  - Parabólicas
  - Dipolos

Access Point (AP)

- Es el punto de acceso de las redes en modo infraestructura
- Forma una red inalámbrica interconectando distintos dispositivos wireless.
- Permite conectarse a otro AP y extender el área de cobertura (Roamming).
- Poseen direcciones IP para ser configurados
- Dependiendo el tipo de antena, cubren desde varios metros hasta varios kilómetros.

Bridges/Repetidores

- Se utilizan para unir dos áreas separadas
- La mayoría de los AP tienen funciones de Bridge/Repetidores



Wireless Cards

- Son los dispositivos que se conectan en el equipo cliente
- Pueden ser:
  - PCMCIA
  - PCI
  - Adaptadores USB
- Algunos tienen la posibilidad de agregar una antena externa

Antenas

- Hay varios tipos de clasificaciones
  - Activas / Pasivas
  - Omnidireccionales / Direccionales

- Dependen de:
  - La frecuencia
  - “Ganancia” (dBi)
  - Angulo de apertura (direccionales)
  - Alcance

- Tipos de antena
  - Yagi
  - Dipolo
  - Parabólica

Mecanismos de Autenticación WEP y WPA

- Para la autenticación de clientes de redes wireless contra un Access Point, existen dos métodos:
  - Autenticación Abierta
  - Autenticación PSK (Pre Shared Key) o por clave compartida

- La autenticación abierta no provee ningún tipo de mecanismo de seguridad, simplemente es un pedido de conexión a la red

- La autenticación por PSK utiliza un mecanismo de desafío-respuesta para autenticar y asociar al cliente a la red.

- El primer agregado de seguridad al estándar 802.11 fue WEP (Wireless Equivalent Privacy).

Autenticación Abierta (Wep / WPA)

- El proceso de autenticación se realiza en texto plano
- No se verifica ni al usuario ni al host, es abierta a cualquiera
- Normalmente está ligada al uso del sistema WEP
- Un cliente puede asociarse al AP con una clave WEP incorrecta o incluso sin una clave WEP, pero no podrá enviar o recibir datos, ya que la carga de paquetes estará encriptada
- Es importante aclarar que el encabezado no está cifrado por WEP, solo la transmisión de los datos lo está

Autenticación por PSK

- Funciona de manera análoga al caso anterior, solo que agrega un paso
- La clave compartida requiere que el cliente y el access point tengan la misma clave WEP

Autenticación por PSK (Cont.)

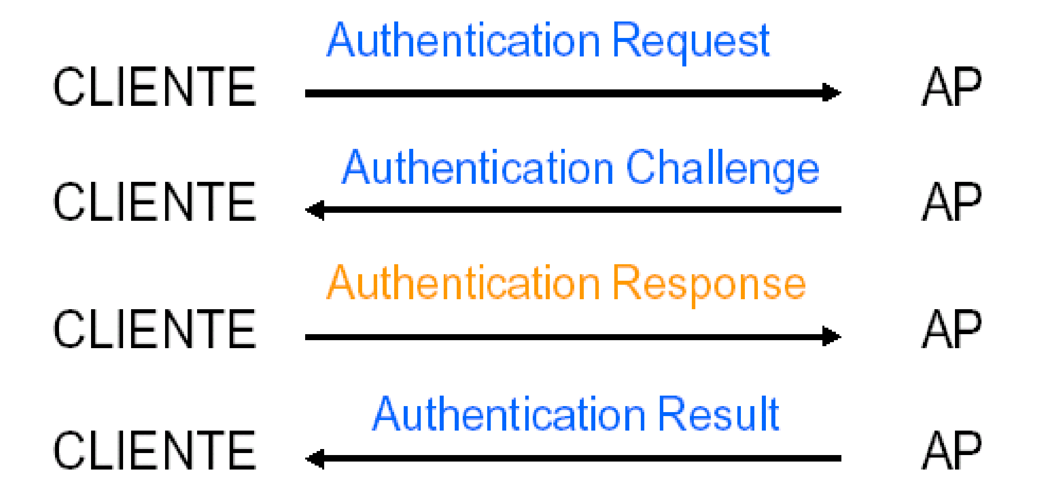
CLIENTE —— Authentication Request ——> AP

CLIENTE <—— Authentication Challenge —— AP

- El equipo que quiere autenticarse (cliente), envía una trama **AUTHENTICATION REQUEST** indicando que quiere utilizar una "clave compartida"

- El destinatario (AP) contesta enviando una trama que contiene 128 octetos de texto (desafío) al cliente.
  - El desafío se genera con la clave compartida y un vector de inicialización (IV) aleatorio utilizando un PRNG (Generador de Números Pseudo Aleatorios)

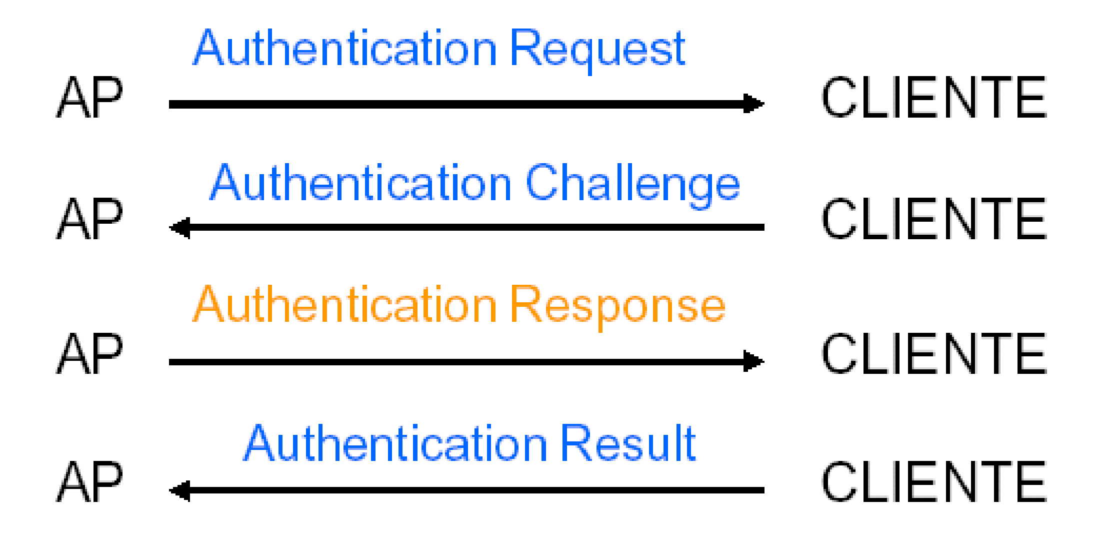
Autenticación por PSK (Cont.)



- Una vez el cliente recibe la trama, copia el contenido del texto de desafío en el payload de una nueva trama que encripta con WEP utilizando la passphrase (clave compartida) y añade un nuevo IV (elegido por el cliente).

- Ya construida esta nueva trama encriptada, el cliente la envía al AP

Autenticación por PSK (Cont.)



- Se vuelve a repetir el proceso pero esta vez el primero que manda la trama con el **AUTHENTICATION REQUEST** es el AP, de esta manera se asegura una autenticación mutua.

Autenticación por Dirección MAC

- No está incluida en las especificaciones del 802.11
- Pero dada su utilidad muchos vendors brindan esa opción
- Esto se realiza mediante una ACL que puede estar en el dispositivo o bien ser validada frente a un servidor externo
- Como contrapartida, para grandes redes, es un trabajo arduo y requiere que la documentación esté constantemente actualizada
- Dado que viajan en texto plano y que son fácilmente modificables, la autenticación por MAC solo es un buen complemento, no se recomienda su uso como el sistema principal de autenticación

WEP

- En 1999 el estándar IEEE 802.11 implementó un sistema de cifrado para redes WLAN denominado Wired Equivalent Privacy (WEP)
- Especificaba una clave de 40 bits, permitiendo ser exportado y usado en todo el mundo aún con las restricciones para la exportación del Gobierno de EEUU
- WEP está basado en el algoritmo simétrico RC4 (Rivest Cipher 4)
- Para utilizar WEP, se debe compartir una clave entre el usuario cliente y el AP

WEP (Cont.)

- Entre las características más importantes de WEP, encontramos:
  - Los mensajes se encriptan junto con un CRC de 32 bits, brindando integridad al sistema
  - La confidencialidad es mantenida por medio de la encripción con RC4
  - Pueden utilizarse claves de 40 bits (incrementadas a 64 bits por medio de un vector de inicialización de 24 bits) o de 104 bits (incrementadas a 128 bits por el mismo IV).
  - Es sencillo de implementar, solo hay que compartir la clave
  - Las características anteriores son la debilidad del método

WEP (Cont.)

- Si bien el ataque trivial a WEP es utilizando Fuerza Bruta, existen una serie de ataques más efectivos.
- Se han desarrollado varios métodos de ataque a este sistema, algunos basados en ataques estadísticos, otros inductivos, etc.
- Algunos de ellos son:
  - Ataque inductivo de Arbaugh
  - Método FMS (Fluhrer-Mantin-Shamir)
  - Su optimización por parte de David Hulton (h1kari)
  - Ataque de KoreK
- Algunas aplicaciones que aprovechan estos métodos para vulnerar WEP son AirSnort, Aircrack o WepLab.

WEP: Evolución de Vulnerabilidades

Fecha	Descripción
Septiembre 1995	Vulnerabilidad RC4 potencial (Wagner)
Octubre 2000	Primera publicación sobre las debilidades de WEP: *Insegura para cualquier tamaño de clave; Análisis de la encapsulación WEP* (Walker)
Mayo 2001	Ataque contra WEP/WEP2 de Arbaugh
Julio 2001	Ataque CRC *bit flipping – Intercepting Mobile Communications: The Insecurity of 802.11* (Borisov, Goldberg, Wagner)
Agosto 2001	Ataques FMS – Debilidades en el algoritmo de programación de RC4 (Fluhrer, Mantin, Shamir)
Agosto 2001	Publicación de AirSnort
Febrero 2002	Ataques FMS optimizados por h1kari
Agosto 2004	Ataques KoreK (IVs únicos) – publicación de chopchop y chopper
Julio/ Agosto 2004	Publicación de Aircrack (Devine) y WepLab (Sánchez), poniendo en práctica los ataques KoreK.

WPA

- Son las siglas de Wi-Fi Protected Access (WPA)
- Es un sistema basado en WEP para proteger las redes inalámbricas que mejora sus aspectos débiles.
- WPA comparte bastantes características con el estándar IEEE 802.11i y fue creado como sistema de transición entre WEP y 802.11i mientras el desarrollo de éste era finalizado.

WPA (Cont.)

- WPA fue diseñado para utilizar un servidor de autenticación (normalmente bajo RADIUS) que permite distribuir claves diferentes a cada usuario, por medio del protocolo 802.1x
- También puede utilizarse en un modo menos seguro, pero más simple, a través de claves compartidas manualmente (PSK)
- Este último es muy utilizados para domicilios y pequeñas empresas y se lo suele denominar WPA personal
- Además incluye protección contra ataques de repetición (replay) a través de un contador para la identificación de las tramas

WPA (Cont.)

Mejoras de WPA respecto a WEP

- Se mejoraron las características de cifrado a partir de la implementación de TKIP
  - TKIP es una implementación mejorada de RC4, aumenta el número de bits de las claves a 128 y las gestiona dinámicamente.
- Se aumentó el número de bits del IV de 24 a 48 bits
  - Se incrementa el espacio de claves
  - Se reduce la reutilización de Ivs
- Permite Autenticación contra un servidor externo
- Se mejoró el chequeo de integridad de la información

WPA (Cont.)

- WPA2 es similar a 802.11i y utiliza AES para cifrar el payload
- Pero WPA2 también permite el uso de TKIP por retrocompatibilidad con tecnologías anteriores.
- AES es considerado como un algoritmo imposible de crackear.
  - Pero para su procesamiento requiere potentes procesadores
  - Dispositivos tales como PDAs, Smartphones, etc no suelen soportarlo

WPA (Cont.)

- WPA y WPA2 Personal utiliza para la autenticación WLANs

- WPA y WPA2 Enterprise autentican a sus usuarios a través de servidores RADIUS utilizando el estándar 802.1x/EAP

- 802.11i y WPA2 utilizan los mismos mecanismos de cifrado y autenticación

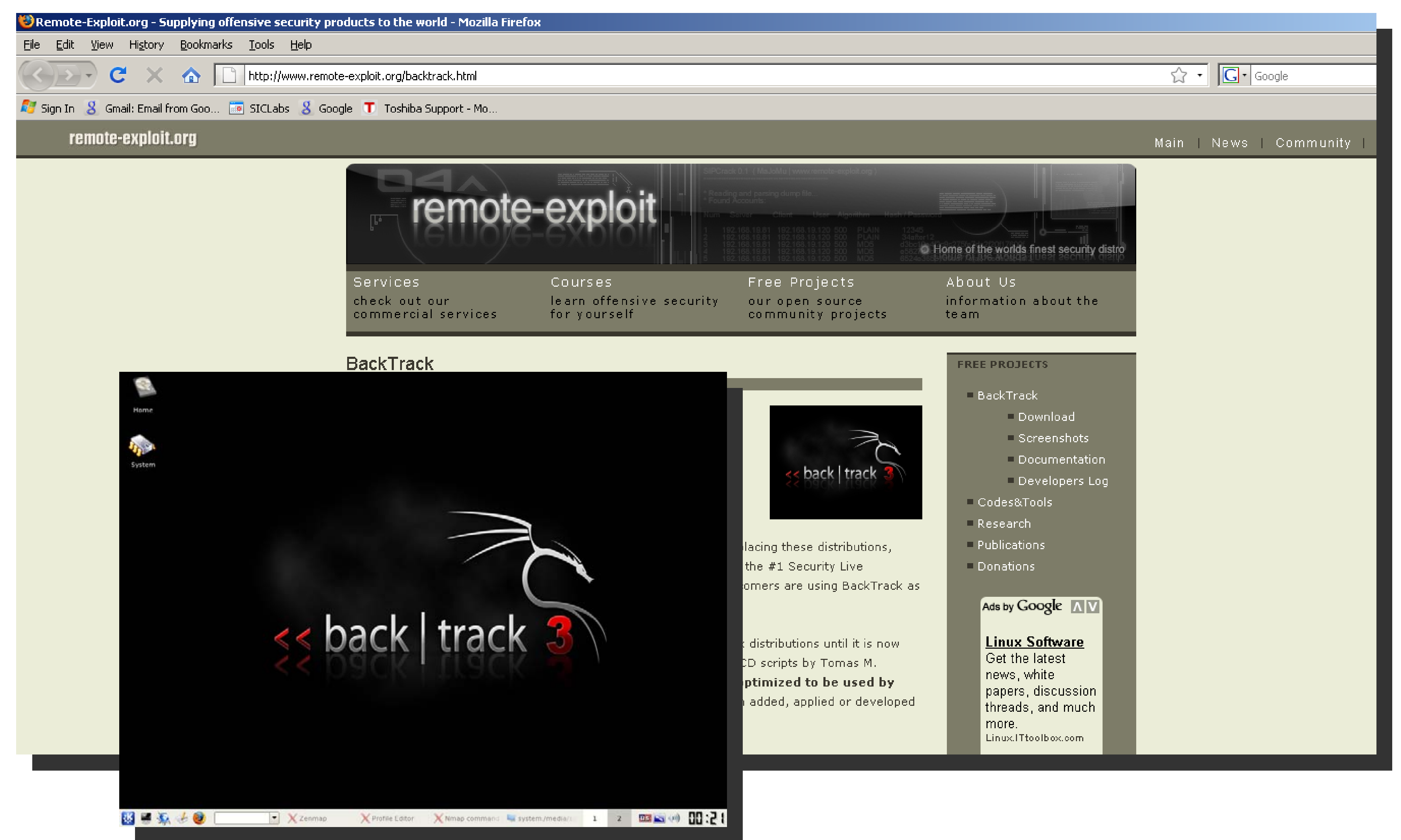
Información Adicional

Método	Cifrado	Autenticación	Debilidad
Estándar IEEE 802.11 original	WEP	WEP	La debilidad de los IV facilita el crackeo de la clave WEP. Se utiliza la misma clave para autenticar a todos los clientes de la red. El CRC utilizado para el chequeo de integridad es una función lineal.
WPA	TKIP	Passpharse o RADIUS (802.1x / EAP)	La passphrase es susceptible de ataques por diccionario o fuerza bruta.
WPA2	AES (por retrocompatibilidad puede usar TKIP)	Passpharse o RADIUS (802.1x / EAP)	La passphrase es susceptible de ataques por diccionario o fuerza bruta.
IEEE 802.11i	AES (por retrocompatibilidad puede usar TKIP)	Passpharse o RADIUS (802.1x / EAP)	La passphrase es susceptible de ataques por diccionario o fuerza bruta.

WEP/WPA

- Herramientas propuestas por CEH:
  - Aircrack
  - Airsnort
  - WEPCrack
  - Kismet
  - Netstumbler
  - SMAC

Herramientas WiFi: Backtrack



Wireless Sniffers y Localización de SSIDs

- Los ataque más comunes a redes inalámbricas incluyen técnicas de sniffing o eavesdropping
- Es un modo sencillo para realizar un ataque sobre redes inalámbricas cuyos APs están configurados por defecto, ya que los paquetes usualmente están sin cifrar.
- Algunas contraseñas de protocolos como FTP, POP3 y SMTP pueden ser capturadas en texto plano por un atacante si la red no está cifrada

Wireless Sniffers y Localización de SSIDs (Cont.)

- Como se vio anteriormente, el SSID se utiliza para identificar distintas redes.
- El SSID es parte de un paquete de gestión (beacon frames) en texto plano.
- Una medida extra de seguridad es ocultar el SSID para que no sea publicado por el AP.
- De todas formas, algunas herramientas pueden identificar el SSID incluso si está oculto.
  - Esto lo hacen sniffeando la red y esperando que un cliente válido pregunte por el nombre de la red que se está intentando ocultar

Rogue Access Point

- Un Rogue Access Point es un dispositivo colocado en la red sin la correspondiente autorización.
  - Por ejemplo un empleado conecta un AP a una boca de red y habilita una red wireless no oficial dentro de la oficina.

- Este AP abre una brecha de seguridad en la red, ya que permitiría que quien se asocie al mismo, salte las restricciones de seguridad propias de la red WiFi oficial.

- Un atacante podría conectar un Rogue AP en la red corporativa y obtener un acceso paralelo a la misma.

- Por esta razón es importante que las organizaciones posean políticas de conectividad inalámbrica que incluyan escaneos de la red wireless periódicos.
  - De esta manera se detectaría cualquier Rogue AP conectado.

Técnicas de Wireless Hacking

- La mayoría de los ataques a redes inalámbricas están definidos por alguna de las siguientes categorías:
  - Mecanismos de autenticación y cracking del cifrado
    - Estos incluyen WEP, WPA PSK, y Lightweight EAP authentication (LEAP) de Cisco.
    - Un atacante puede conectarse a la WLAN utilizando credenciales robadas o capturando tráfico de otros usuarios válidos y crackeando el cifrado.
  - Eavesdropping o sniffing
    - Implica capturar contraseñas u otro tipo de inforamción confidencial a partir de una WLAN no cifrada

Técnicas de Wireless Hacking (Cont.)

- **Denegación de Servicio**
  - Un ataque de DoS puede realizarse desde la capa física del modelos OSI (capa 1) utilizando dispositivos que generan una fuerte interferencia de RF, imposibilitando a los clientes conectarse a él. Esta técnica se denomina jamming.

  - También puede llevarse a cabo desde la capa de enlace (capa 2), más precisamente la capa LLC, a partir de la generación de paquetes de desautenticación (Deauth atack) o por la generación continua de paquetes bogus (Queensland attack)

Técnicas de Wireless Hacking (Cont.)

- **Enmascaramiento de AP o spoofing**
  - Los Rogue APs pretenden hacerse pasar por AP legítimos y hacer que los clientes se conecten a ellos.
  - De esta manera, el cliente utiliza sus credenciales válidas en el AP falso. Karma es una herramienta que realiza esto.

- **MAC spoofing**
  - Un atacante podría saltear la autenticación por MAC
  - El atacante falsifica la dirección utilizando una dirección válida, de esta manera saltea el filtro MAC

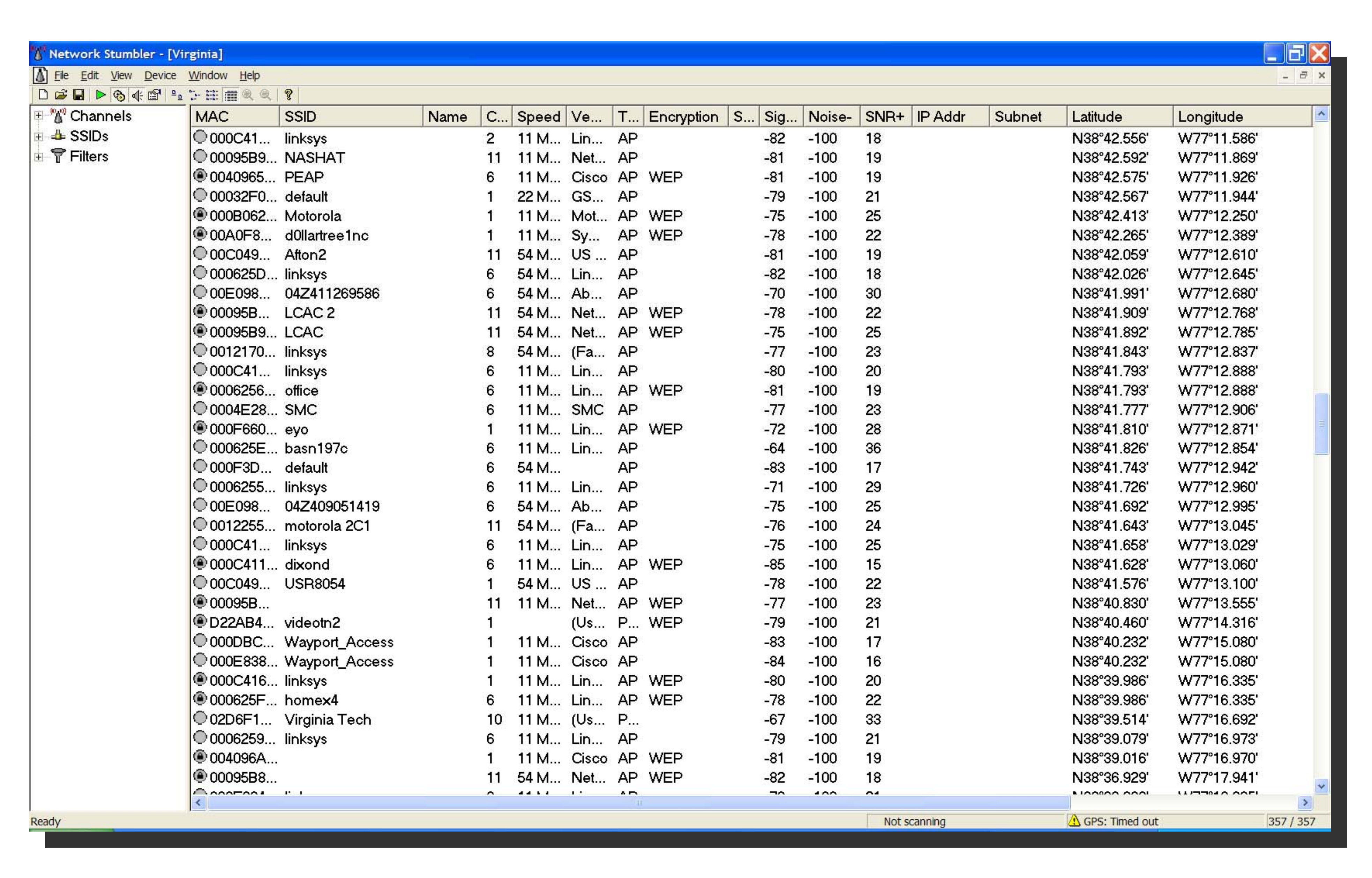
Ataque a una WLAN

- Paso 1: Buscar redes para atacar
- Paso 2: Seleccionar una red para atacar
- Paso 3: Analizar la red
- Paso 4: Craquear la clave WEP
- Paso 5: Sniffear la red

Ataque a una WLAN (Cont.)

- **Paso 1: Buscar redes para atacar**
  - Un atacante debe utilizar primero NetStumbler o herramienta similar para obtener un mapa de las redes wireless activas.
  - Utilizando Netstumbler, el atacante localiza señales de una WLAN.
  - Netstumbler no solo tiene la habilidad de monitorear todas las conexiones de red activas en un área, también puede ser integrado con un GPS para mapear los access point.

Ataque a una WLAN (Cont.)

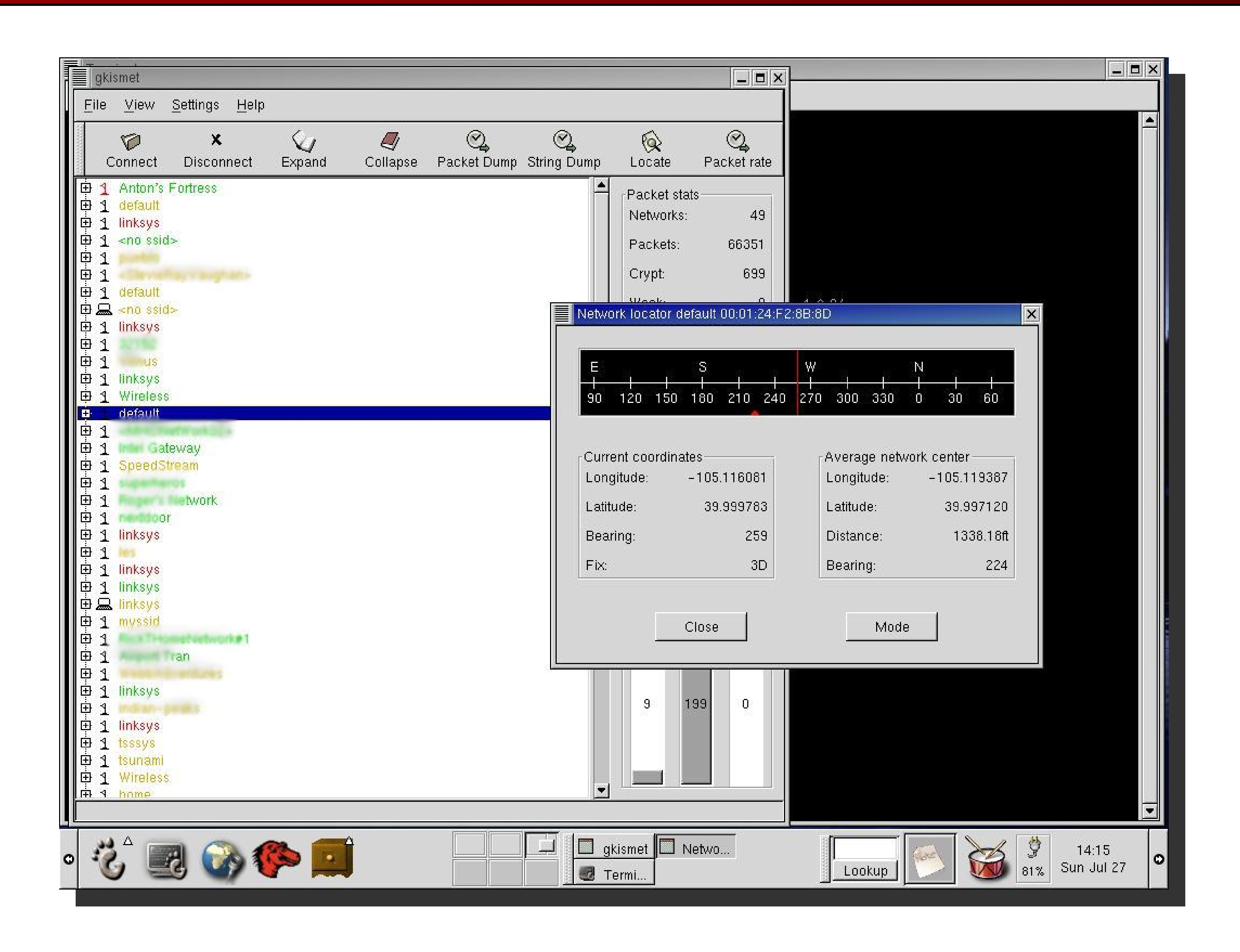


MAC	SSID	Name	C...	Speed	Ve...	T...	Encryption	S...	Sig...	Noise-	SNR+	IP Addr	Subnet	Latitude	Longitude
000C41...	linksys		2	11 M...	Lin...	AP			-82	-100	18			N38°42.556'	W77°11.586'
00095B9...	NASHAT		11	11 M...	Net...	AP			-81	-100	19			N38°42.592'	W77°11.869'
0040965...	PEAP		6	11 M...	Cisco	AP	WEP		-81	-100	19			N38°42.575'	W77°11.926'
00032F0...	default		1	22 M...	GS...	AP			-79	-100	21			N38°42.567'	W77°11.944'
000B062...	Motorola		1	11 M...	Mot...	AP	WEP		-75	-100	25			N38°42.413'	W77°12.250'
00A0F8...	d0llartree1nc		1	11 M...	Sy...	AP	WEP		-78	-100	22			N38°42.265'	W77°12.389'
00C049...	Afton2		11	54 M...	US ...	AP			-81	-100	19			N38°42.059'	W77°12.610'
000625D...	linksys		6	54 M...	Lin...	AP			-82	-100	18			N38°42.026'	W77°12.645'
00E098...	04Z411269586		6	54 M...	Ab...	AP			-70	-100	30			N38°41.991'	W77°12.680'
00095B...	LCAC 2		11	54 M...	Net...	AP	WEP		-78	-100	22			N38°41.909'	W77°12.768'
00095B9...	LCAC		11	54 M...	Net...	AP	WEP		-75	-100	25			N38°41.892'	W77°12.785'
0012170...	linksys		8	54 M...	(Fa...	AP			-77	-100	23			N38°41.843'	W77°12.837'
000C41...	linksys		6	11 M...	Lin...	AP			-80	-100	20			N38°41.793'	W77°12.888'
0006256...	office		6	11 M...	Lin...	AP	WEP		-81	-100	19			N38°41.793'	W77°12.888'
0004E28...	SMC		6	11 M...	SMC	AP			-77	-100	23			N38°41.777'	W77°12.906'
000F660...	eyo		1	11 M...	Lin...	AP	WEP		-72	-100	28			N38°41.810'	W77°12.871'
000625E...	basn197c		6	11 M...	Lin...	AP			-64	-100	36			N38°41.826'	W77°12.854'
000F3D...	default		6	54 M...		AP			-83	-100	17			N38°41.743'	W77°12.942'
0006255...	linksys		6	11 M...	Lin...	AP			-71	-100	29			N38°41.726'	W77°12.960'
00E098...	04Z409051419		6	54 M...	Ab...	AP			-75	-100	25			N38°41.692'	W77°12.995'
0012255...	motorola 2C1		11	54 M...	(Fa...	AP			-76	-100	24			N38°41.643'	W77°13.045'
000C41...	linksys		6	11 M...	Lin...	AP			-75	-100	25			N38°41.658'	W77°13.029'
000C411...	dixond		6	11 M...	Lin...	AP	WEP		-85	-100	15			N38°41.628'	W77°13.060'
00C049...	USR8054		1	54 M...	US ...	AP			-78	-100	22			N38°41.576'	W77°13.100'
00095B...			11	11 M...	Net...	AP	WEP		-77	-100	23			N38°40.830'	W77°13.555'
D22AB4...	videotn2		1		(Us...	P...	WEP		-79	-100	21			N38°40.460'	W77°14.316'
000DBC...	Wayport_Access		1	11 M...	Cisco	AP			-83	-100	17			N38°40.232'	W77°15.080'
000E838...	Wayport_Access		1	11 M...	Cisco	AP			-84	-100	16			N38°40.232'	W77°15.080'
000C416...	linksys		1	11 M...	Lin...	AP	WEP		-80	-100	20			N38°39.986'	W77°16.335'
000625F...	homex4		6	11 M...	Lin...	AP	WEP		-78	-100	22			N38°39.986'	W77°16.335'
02D6F1...	Virginia Tech		10	11 M...	(Us...	P...			-67	-100	33			N38°39.514'	W77°16.692'
0006259...	linksys		6	11 M...	Lin...	AP			-79	-100	21			N38°39.079'	W77°16.973'
004096A...			1	11 M...	Cisco	AP	WEP		-81	-100	19			N38°39.016'	W77°16.970'
00095B8...			11	54 M...	Net...	AP	WEP		-82	-100	18			N38°36.929'	W77°17.941'

Ataque a una WLAN (Cont.)

- **Paso 2: Seleccionar una red para atacar:**
  - En este punto, el atacante ya selecciono un objetivo.
  - NetStumbler o Kismet pueden decirle si la red esta cifrada o no.

Ataque a una WLAN (Cont.)



Ataque a una WLAN (Cont.)

- **Paso 3: Analizar la red:**
  - Determinar si:
    - La WLAN no realiza broadcasting de SSID.
    - NetStumbler identifica el SSID.
    - Múltiples access points están presentes.
    - Método de autenticación abierto.
    - La WLAN esta cifrada con WEP de 40bit.
    - La WLAN no esta utilizando 802.1X.

Ataque a una WLAN (Cont.)

- **Paso 4: Craquear la clave WEP:**
  - El atacante configura la interface Wireless en modo monitor.
  - Luego captura paquetes con Airodump.
  - Airodump lista las redes disponibles con su SSID e inicia la captura de paquetes.
  - Después de algunas horas capturando con Airodump, lanza Aircrack para iniciar el cracking.
  - La clave WEP es revelada.

Ataque a una WLAN (Cont.)

- **Paso 5: Sniffear la red:**
  - Una vez que la clave WEP es revelada y la WNIC es configurada correctamente, una IP le es asignada al atacante y ahora puede acceder a la WLAN.
  - El atacante puede sniffear trafico con Ethereal.
  - Puede realizar un Sniffing de los protocolos en texto plano como FTP, POP o Telnet en busca de contraseñas.

Obtención de Clave WEP Bajo Linux

- En entornos linux, con aircrack-ng y aircrack-ptw, en una serie de 5 pasos se puede obtener una clave WEP con suma facilidad.

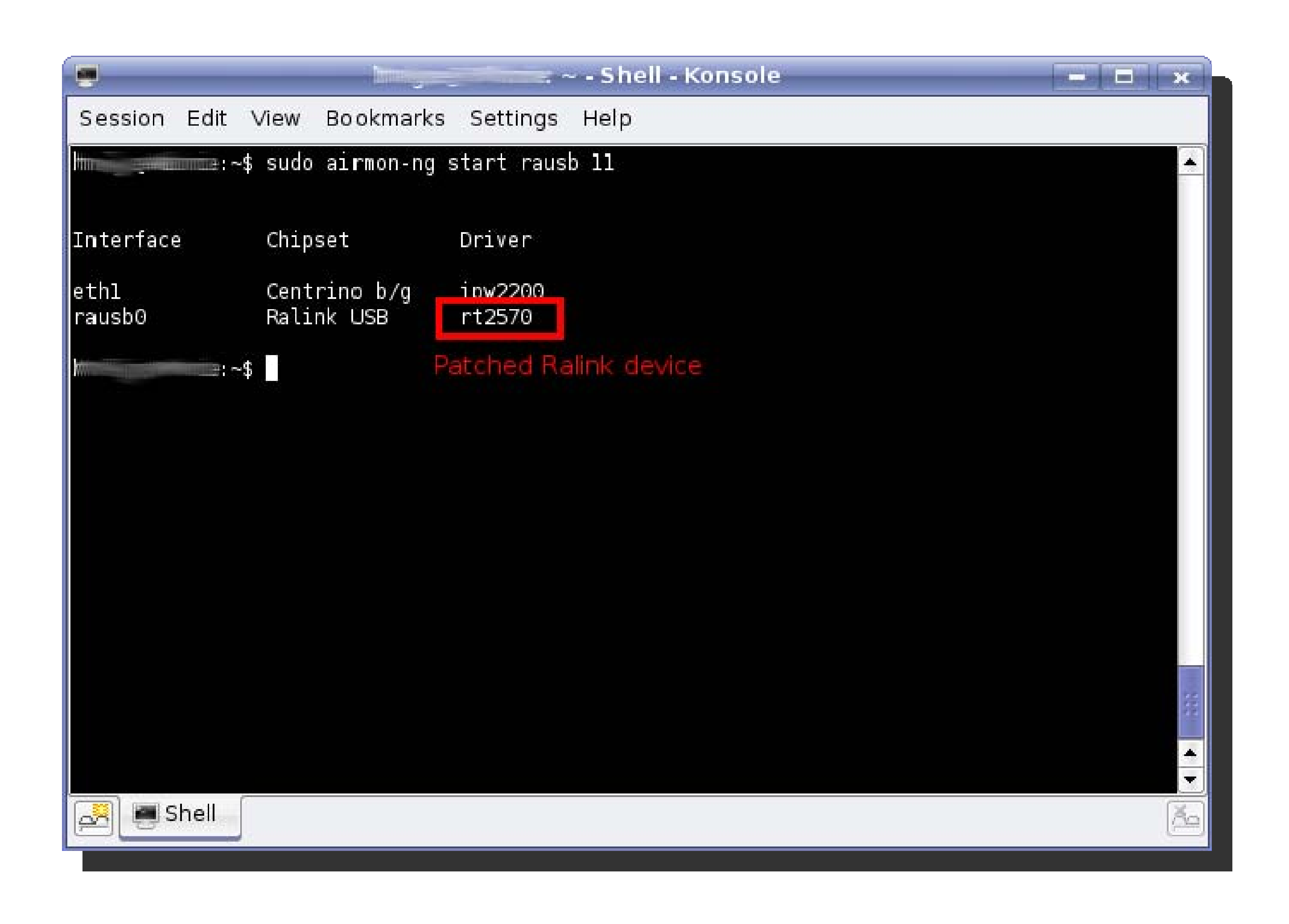
1. Habilitando modo monitor con `airmon-ng`
2. Captura de paquetes con `airodump-ng`
3. Determinación de filtrado MAC
   - Desautenticación con `aireplay-ng`*
4. Re-inyección con `aireplay-ng`
5. Decryption with `aircrack-ng` & `aircrack-ptw`

*Si existe filtrado por MAC

Obtención de Clave WEP Bajo Linux (Cont.)

1. Habilitando modo monitor con "airmon-ng"

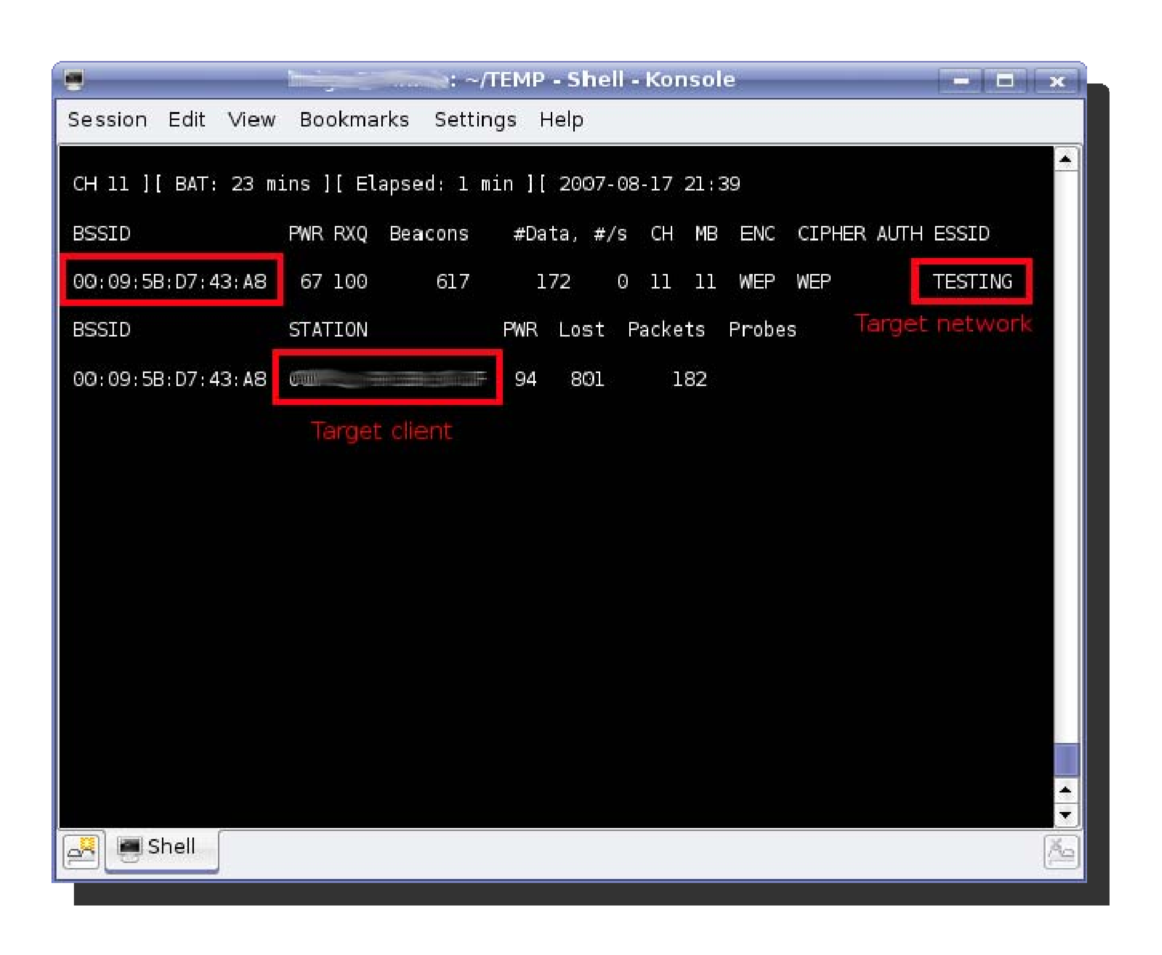
```
# airmon-ng start <interfase> <canal>
```



Obtención de Clave WEP Bajo Linux (Cont.)

2. Captura de paquetes con "airodump-ng"

```
# airodump-ng --channel <canal> --bssid
     MAC_objetivo --write <capturas> <interfase>
```



Obtención de Clave WEP Bajo Linux (Cont.)

3. Determinación de filtrado MAC

```
# aireplay-ng -1 0 -e <SSID_objetivo> -a
   MAC_objetivo -h MAC_spoofeada <interfase>
```

Si se obtiene un resultado como el mostrado a continuación, no existe filtrado de dirección MAC.

```
18:22:32 Sending Authentication Request
18:22:32 Authentication successful
18:22:32 Sending Association Request
18:22:32 Association successful :-)
```

En ese caso, se saltea el paso de des-autenticación.

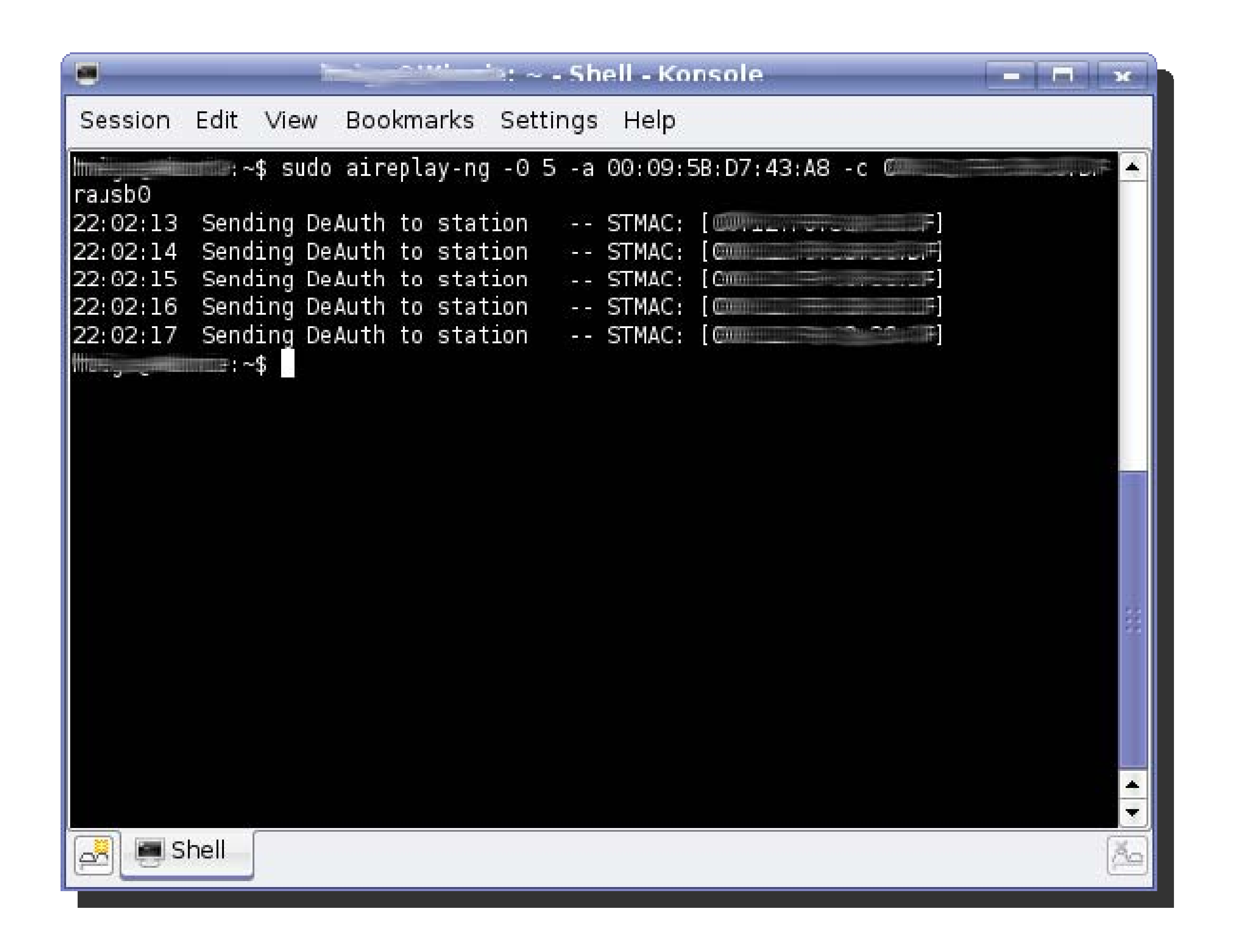
Obtención de Clave WEP Bajo Linux (Cont.)

- Desautenticación con "aireplay-ng“

```
# aireplay-ng -0 5 -a MAC_objetivo -c
MAC_spoofeada   <interfase>
```

Al existir filtrado por direcciones MAC, la `MAC_spoofeada` debe ser la dirección MAC de un cliente válido.

Obtención de Clave WEP Bajo Linux (Cont.)



Obtención de Clave WEP Bajo Linux (Cont.)

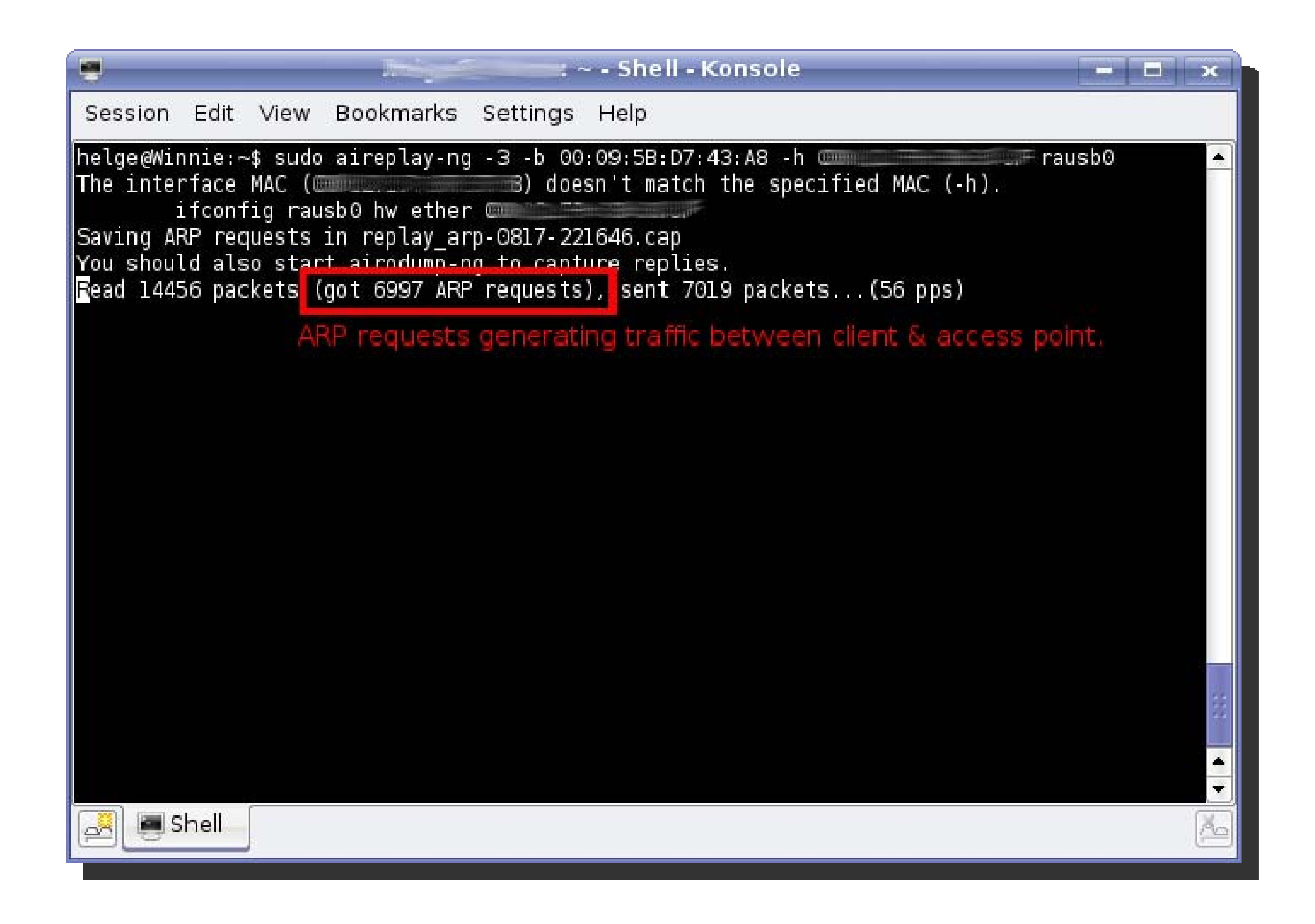
4. Re-inyección con "aireplay-ng“

```
# aireplay-ng -3 -b MAC_objetivo -h MAC_spoofeada
    <interfase>
```

Si no existe filtrado por direcciones MAC, la `MAC_spoofeada` puede ser cualquier dirección MAC.

Si existe filtrado por direcciones MAC, la `MAC_spoofeada` debe ser la dirección MAC de un cliente válido.

Obtención de Clave WEP Bajo Linux (Cont.)



Obtención de Clave WEP Bajo Linux (Cont.)

5. Crackeo del password con "aircrack-ng" y "aircrack-ptw"

```
# aircrack-ng <capturas>.cap
```

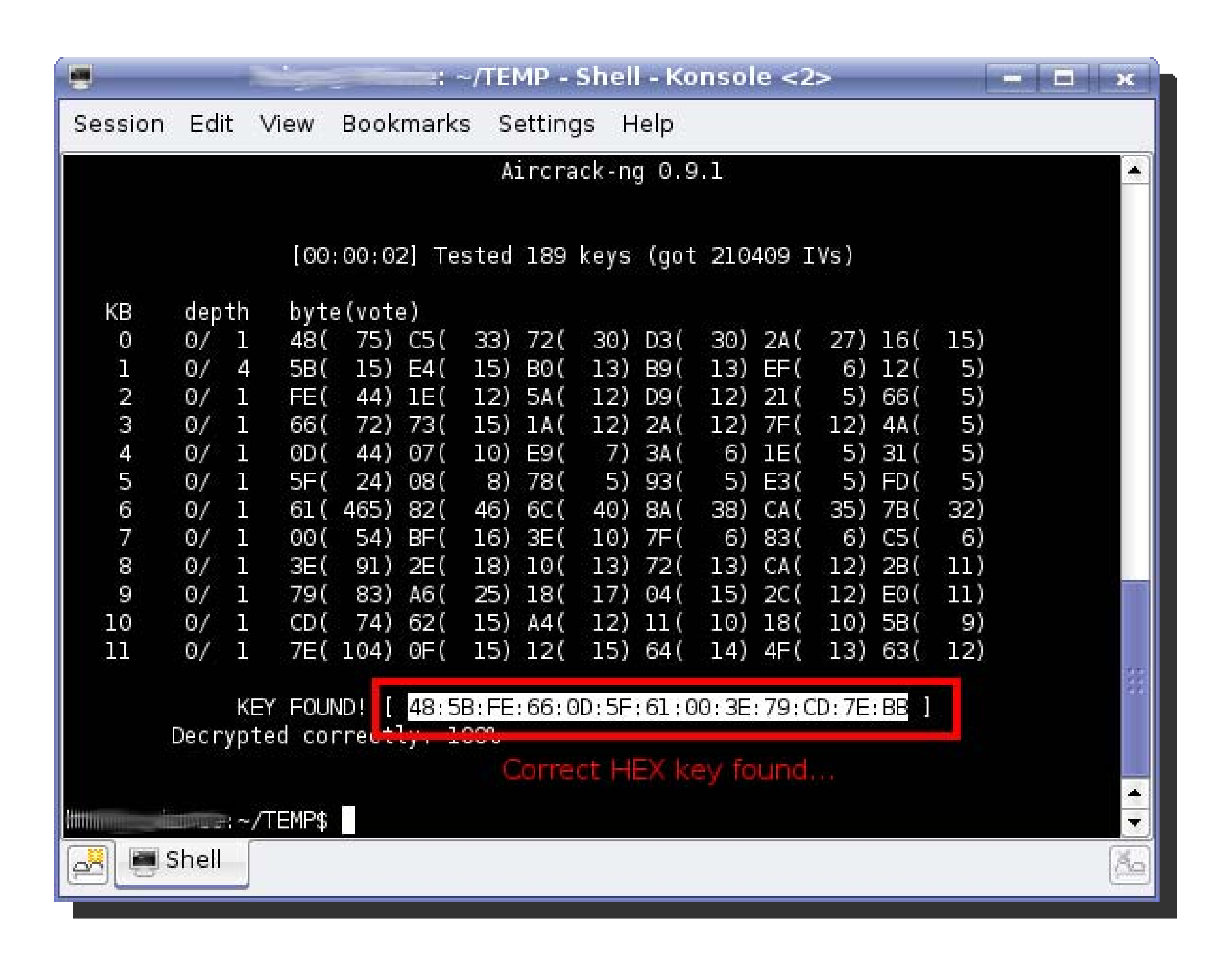
```
# ./aircrack-ptw <capturas>.cap
```

La diferencia entre aircrack-ng y aircrack-ptw radica en la cantidad de paquetes que requiere capturar cada herramienta. A continuación se detalla esto:

```
Aircrack-NG:
64-bit key: ~250,000 paquetes
128-bit key: ~1,500,000 paquetes

Aircrack-PTW:
64-bit key: ~20,000 paquetes [estimado]
128-bit key: ~85,000 paquetes
```

Obtención de Clave WEP Bajo Linux (Cont.)



Métodos de Securización

- Los métodos utilizados para securizar una red wireless pueden ser caracterizados según las capas del modelo OSI.

- Para la Capa 2 (capa de enlace):
  - WPA
  - WPA2
  - 802.11i

- Para la Capa 3 (capa de red)
  - IPSec
  - SSL VPN

- Para la Capa 7 (capa de aplicación)
  - Utilizar protocolos o aplicaciones seguras tal como:
    - Secure SHell (SSH)
    - HTTP Over SSL (HTTPS)
    - FTP/SSL (FTPS)

Métodos de Securización (Cont.)

- A continuación se detallan algunos métodos complementarios de seguridad.
  - Autenticación por dirección MAC
  - Esconder el SSID
  - Usar claves fuertes
    - Set de caracteres alfanuméricos
    - Mayúsculas y minúsculas
    - Caracteres especiales (@, $, #, . , etc)

Wireless Hacking

Links, Referencias y
Lecturas Complementarias

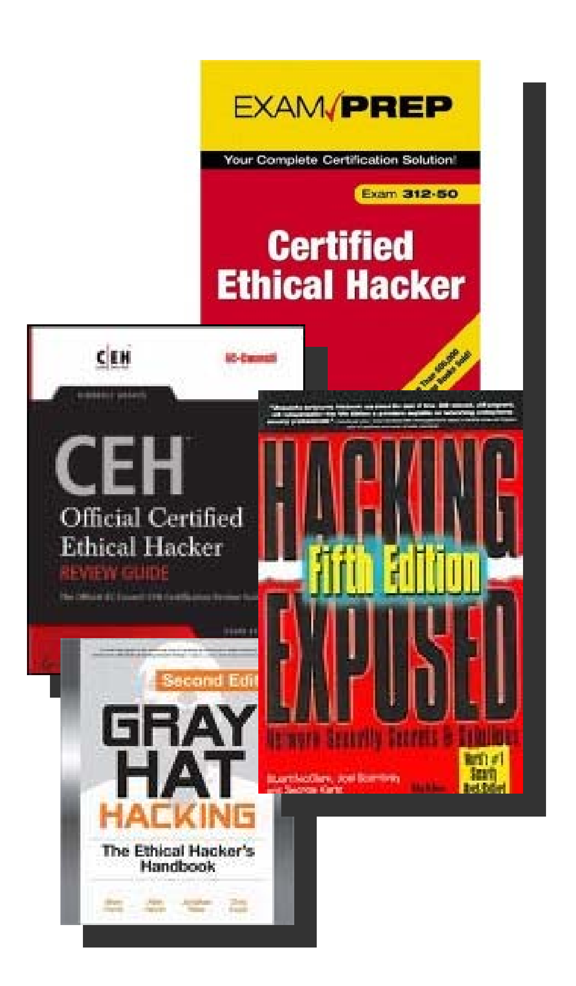
Links

- NetStumbler - http://www.netstumbler.com/
- AirSnort - http://airsnort.shmoo.com/
- Kismet - http://www.kismetwireless.net/
- Aircrack-NG - http://www.aircrack-ng.org/
- Aircrack-PTW - http://www.wirelessdefence.org/Contents/Aircrack-ptw.htm
- BackTrack 3 - http://www.remote-exploit.org/
- WiFi Slax - http://www.wifislax.com/
- Diferencias entre aircrack-ng y aircrack-ptw

  http://www.wirelessdefence.org/

Referencias y Lecturas Complementarias

- **CEH Official Certified Ethical Hacker Review Guide**
  By Kimberly Graves
  (Sybex) ISBN: 0782144373
- **Certified Ethical Hacker Exam Prep**
  By Michael Gregg
  (Que) ISBN: 0789735318
- **Hacking Exposed, Fifth Edition**
  By S.McClure, J.Scambray, and G.Kurtz
  (McGraw-Hill Osborne Media) ISBN: 0072260815
- **Gray Hat Hacking, Second Edition**
  By S.Harris, A.Harper, C.Eagle, J.Ness
  (McGraw-Hill Osborne Media) ISBN: 0071495681



Wireless Hacking

Preguntas?